

**IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF MONTANA**

**IN THE MATTER OF THE
SEARCH OF:**

**The cellular telephone
answering to phone number
(630) 398-9001**

Case No. MJ-22-12-BLG-TJC

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH
WARRANT**

I, Ryan Hammer, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Fed. R. Crim. P. 41 for a search warrant authorizing the search of a cellular telephone answering to phone number (630) 398-9001, further described in Attachment A, for evidence and instrumentalities concerning violations of Title 18, United States Code, Section 875(c), transmitting in interstate commerce communications containing a threat to injure the person of another as described in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since June of 2016. I am permanently assigned to the San Antonio Division, McAllen Resident Agency (RA) but am currently assigned to the Salt Lake City Division, Billings RA on a Temporary Duty Travel

(TDY). I attended the FBI Academy in Quantico, Virginia, which entailed 21 weeks of training in law enforcement and investigative activities. In the performance of my duties, I have investigated and assisted in the investigation of violent criminal organizations to include home invasion crews, gangs, drug trafficking organizations, kidnappings, and assaults on federal officers. In that capacity, I have taken part in cooperating witness interviews, cooperating defendant interviews, and debriefings with confidential human sources. I have received training from the FBI pertaining to the investigation of such matters to include training on cellphone analysis as well as social media accounts and their analysis. In addition, I have conferred with FBI colleagues with extensive training and experience in the investigation of criminal organizations. The information contained in this affidavit is based on my own observations, training and experience and information provided to me by other task force members or other law enforcement officers.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. In my training and experience, examining data stored on smartphone devices can uncover, among other things, evidence of who possessed or used the

device, who the user was communicating with, and the content of those communications. Based on my knowledge, experience and training, I believe that the person who was using the phone, may have committed acts consistent with transmitting in interstate commerce communications containing a threat to injure the person of another, as defined in 18 U.S.C. 875(c). The applied for search warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the

location of the device.

- b. **Data:** means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.
- c. **Email or electronic mail:** means messages transmitted over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Most mainframes, computer networks, and minicomputers have an email system. Sent messages are stored in electronic mailboxes at least until the recipient retrieves them. After reading electronic mail, recipients can store it on their computer as a file, forward it to other users, or delete it, or they may store the message on a remote server, such as the one from which they may have retrieved the email.
- d. **Image or copy:** refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.
- e. **Internet:** is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. **Text Messages:** are a form of communication through the use of cellular telephones or handheld electronic devices upon an electronic service provider’s network or system. A message normally contains text composed by the sender, usually input via a lettering system on the device or computers keypad. The message can also be an image or short video sent or received.
- g. **Uniform Resource Locator:** (URL) *are typically used to access web*

sites or other services on remote devices such as <http://www.usdoj.gov>, for example.

- h. **Voice Mail:** means a computerized system for answering incoming phone calls and allowing the caller to leave a message, which may be later retrieved.
- i. **World Wide Web:** can be considered a massive database of information that is stored on linked computers that make up the Internet. This information can be displayed on a computer in the form of a web page, which is a document on the World Wide Web. A web site is a related collection of files and can consist of any number of web pages.

6. Based on my training, experience, and research, I know that smartphone devices, such as the device, have capabilities that allow them to serve as a wireless telephone, data storage device, and digital camera and that smartphone devices can connect to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, who the user was communicating with, and the content of those communications. I also know the device would allow to store text messages and digital images of, or related to, the possession or distribution of controlled substances or firearms.

7. Based upon my knowledge, training, and experience in investigating federal crimes, and the experience and training of other law enforcement officers with whom I have had discussions, I am aware of the following:

EXAMINATION OF ELECTRONICAL INFORMATION

8. The examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the United States needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant.

9. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders responsive to this search warrant do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

10. If the examination does not reveal any data falling within the scope of the warrant, the United States will seal any non-responsive information, absent further authorization from the Court.

11. The United States will retain a forensic image of all of the electronic information produced during the examination of the device to prove the authenticity of evidence to be used at trial, to respond to questions regarding the corruption of data, to establish a chain of custody of data, to refute claims of

fabricating, tampering, or destroying data, and to address potential exculpatory evidence claims where, for example, a defendant claims that the United States avoided its obligations by destroying data or returning it to a third party.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

12. It is not possible to determine, merely by knowing the smartphone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Smartphone devices today can be simple cellular telephones and text message devices, and/or they can include cameras, serve as personal digital assistants and have functions such as calendars and full address books, and/or they can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the devices may only be powered in a secure environment or, if possible, started in "airplane mode," which disables access to the network. Unlike typical computers, many smartphones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some smartphone models using forensic hardware and software. Even if some of the stored

information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive.

13. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, items that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

14. Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), I seek permission for an agent review of the device as well as the forensic examination of the device consistent with the warrant. The examination will require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

15. In searching the data stored on the device, law enforcement personnel executing this search warrant will employ the following procedure:

- a. The team searching the device will do so only by using search protocols specifically chosen to identify only the specific items to be seized described in Attachment B.
- b. The team may subject all of the data contained in the device or the forensic copy to the protocols to determine whether the device and any data falls within the items to be seized described in Attachment B. The team searching the device may also search for and attempt to recover “deleted,” “hidden” or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized described in Attachment B.
- c. These search protocols also may include the use of tools to exclude normal operating system files and standard third-party software that do not need to be searched.
- d. When searching the device pursuant to the specific search protocols selected, the team searching the device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.
- e. If the team searching the device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.
- f. At the conclusion of the search of the device, any one device determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the United States until further order of the Court or one year after the conclusion of the criminal case/investigation.
- g. Notwithstanding, after the completion of the search of the device, the United States shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained device or digital data absent further order of Court.

- h. If the search team determines that a device is not an instrumentality of any offense under investigation and does not contain any data falling within the list of items to be seized described in Attachment B, the United States will as soon as practicable return the device and delete or destroy all the forensic copies thereof.
- i. If the search determines that the device or the forensic copy is not an instrumentality of any offense under investigation but does contain data falling within the list of the items to be seized described in Attachment B, the United States either (i) within the time period authorized by the Court for completing the search, return to the Court for an order authorizing retention of the device and forensic copy; or (ii) retain only a copy of the data found to fall within the list of the items to be seized described in Attachment B and return the device and delete or destroy all the forensic copies of the device.

PROBABLE CAUSE

16. As set forth in more detail below, on January 20, 2022, Thomas Bennett called a 911 dispatcher located in Oak Lawn, Illinois, using the Subject Phone, and threatened to murder ‘Victim A.’ At the time he made the January 20 call from the Subject Phone, Bennett was located in or around Bozeman, Montana. Following this January 20, 2022 call, Bennett left numerous additional voicemails for Individual A at Individual A’s place of business in which Bennett described Individual A as “f***ed” and other individuals as “f***ed.”

17. According to information received from the Oak Lawn, Illinois, Police Department Central Dispatch, which receives 911 calls for the Evergreen Park Police Department (EPPD), at 2:22 a.m. on January 20, 2022, a male, who identified

himself in the call as “Thomas R. Bennett,” called the Oak Lawn Police Department Central Dispatch from telephone number (630) 398-9001 (the Subject Phone).

18. FBI Task Force Officer (TFO) Chris LeCompte conducted a review of that call, which was recorded, and determined the following: Bennett told the dispatcher that he was “in the Rockies” where it was “freezing cold” and demanded that the dispatcher tell him who was the “shot caller in Evergreen Park.” Later in the call, Bennett asked about two individuals: “Victim A” and “Victim B.” Bennett stated that “Victim A is a n***er, he’s a f***k face, he is getting murdered. I’m going to murder him with my bare hands, he’s f***ed.” Bennett then spelled out Victim A’s first name for the dispatcher. Bennett then asked the dispatcher “Does Victim A still work there?” Later in the call, Bennett asked the dispatcher again: “So, can you just do me a favor, have somebody find out, does this f***ing n***er Victim A still work there?” Bennett continued: “. . . and so Victim B’s f***ed because apparently one of his nephews was in the naval academy . . . he’s f***ed.” Bennett also spelled out Victim B’s last name for the dispatcher.

19. FBI TFO LeCompte knows that Victim A is an EPPD officer, and Victim B is a former EPPD officer.

20. According to information and records obtained from EPPD, following the call by Bennett, EPPD obtained records from AT&T, the service provider for

Bennett's Phone. According to those records, at the time Bennett called the EPPD police dispatch, the Subject Phone was located in the state of Montana.

21. According to reports and information from the United States Marshals' Service (USMS), on January 25, 2022, USMS deputies interviewed a relative of Bennett who stated that Bennett had been in Bozeman, Montana, but that to that relative's knowledge, Bennett had traveled back to Chicago by bus on Sunday evening (January 23, 2022).

22. According to reports and information received from the USMS and Individual A's place of business, on January 20 and 23, 2022, an individual identifying himself as "Tom Bennett" called Individual A at Individual A's place of business and left threatening voicemails. According to call logs maintained by Individual A's place of business, the individual identifying himself as "Tom Bennett" called from telephone number (630) 398-9001 (the Subject Phone) in the early morning hours of January 20, 2022, and the late evening hours of January 23, 2022, and left a total of 7 voicemails.

23. In one of the January 20 voicemails, the individual, who identified himself as both "Thomas R. Bennett" and "Tom Bennett," stated that his phone number was (630) 398-9001 (the Subject Phone) and that his date of birth was June **, 19**, which, according to law enforcement databases, is Bennett's date of birth.

In that January 20 voicemail, Bennett said to Individual A: “buddy, you’re not my buddy, you’re f***ed . . . you are beyond f***ed you mother***er” and that another individual, Individual C, is “f***ed.”

24. Further, on January 23, 2022, this same individual left additional voicemails for Individual A at Individual A’s place of business. According to call logs maintained by Individual A’s place of business, the individual made each call from telephone number (630) 398-9001 (the Subject Phone). In one of the voicemails the caller identified himself as “Tom Bennett.” Based on TFO LeCompte’s review of the voicemails left on January 20 and January 23, 2022, the voice of the caller is the same as that of the individual who made the January 20, 2022 call to Oak Lawn Police Dispatch as described above.

25. According to location information obtained pursuant to a warrant issued by the Circuit Court of Cook County, on January 26, 2022 and as of the morning of January 27, 2022, the Subject Phone was located in or around Billings, Montana.

26. Based upon my training and experience, as well as my experience in this investigation as described above, I know that cellular phones may contain relevant evidence of threatening statements, including call logs as well as text messages documenting communications made or received from the Subject Phone

that are located in the memory of the Subject Phone, which communications may provide evidence of the Subject Offense. Moreover, digital photographs and other data located in the memory of the Subject Phone may contain images of the user of the Subject Phone, places frequented by the user of the phone leading up to and during the Subject Offense, and locations and instrumentalities used in committing the Subject Offense.

27. In addition, based on my training and experience, I know that information stored within a cellular phone may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within a cellular phone can indicate who has used or controlled the cellular phone. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the cell phone at a relevant time. Further, such stored electronic data can show how and when the cell phone and its related account were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cell

phone access, use, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cell phone account owner.


28. Additionally, information stored within a cellular phone may indicate the geographic location of the cell phone and user at a particular time (e.g., location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Stored electronic data may also provide relevant insight into the cell phone owner’s state of mind as it relates to the offense under investigation. For example, information in the cell phone may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the cell phone itself or by a program that deletes or over-writes the data contained within the cell phone, such data will remain stored within the cell phone indefinitely.

29. Because, as explained above, the Subject Phone is associated with the target in this case, there is probable cause to believe the subject phone, described further in Attachment A, contains evidence of the crime of transmitting threats to injure the person of another in interstate commerce.

CONCLUSION


30. Based on the foregoing, I request that the Court issue the proposed search warrant.

RESPECTFULLY SUBMITTED:



Ryan Hammer
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 27 day of January, 2022.



Honorable Timothy J. Cavan
United States Magistrate Judge